

Security

[Security](#) refers to the protection of hardware, software, machines and networks from unauthorized access, alteration or destruction. Security measures include restricted access to machines and networks and encryption of information. The degree of security of information systems determines society's confidence in the information contained in the systems.

Security Measures



Access & Access permissions

Access is just that, being able to get to computers, [Networks](#) and network resources. Access permissions is provided by the sysadmin and the organisation in the form of a password and username. Then the sysadmin provides access through managing 'rights' to the resources that are provided on a network. Resources include files and folders, [Internet](#) & [Intranet](#), printing and much more.

There is an ability to implement different levels of access according to the level of security for personnel. Typically the finance department would have access to the financial files but the secretary may not. At school teachers have access to your grades but students do not.

Physical Barriers

- Restricting access to 'live' Ethernet connections to a network backbone in closed off areas
 - This is simply stopping people getting into an area and require authentication through a key, ID card or biometric scanners.
- Smart cards or ID cards

What is a "smart card"?

A smart card resembles a [credit card](#) in size and shape, but inside it is completely different. First of all, it *has* an inside -- a normal credit card is a simple piece of plastic. The inside of a smart card usually contains an **embedded microprocessor**. The [microprocessor](#) is under a gold contact pad on one side of the card. Think of the microprocessor as *replacing* the usual magnetic stripe on a credit card or debit card.

Smart cards are much more popular in Europe than in the United States. In Europe, the health insurance and [banking](#) industries use smart cards extensively. *Every* German citizen

has a smart card for health insurance. Even though smart cards have been around in their modern form for at least a decade, they are just starting to take off in the United States. Magnetic stripe technology remains in wide use in the United States. However, the data on the stripe can easily be read, written, deleted or changed with off-the-shelf equipment. Therefore, the stripe is really not the best place to store sensitive information. To protect the consumer, businesses in the U.S. have invested in extensive online mainframe-based computer networks for verification and processing. In Europe, such an infrastructure did not develop -- instead, the card carries the intelligence.

The microprocessor on the smart card is there for **security**. The host computer and card reader actually "talk" to the microprocessor. The microprocessor enforces access to the data on the card. If the host computer read and wrote the smart card's random access memory ([RAM](#)), it would be no different than a [diskette](#).

Smarts cards may have up to 8 [kilobytes](#) of RAM, 346 kilobytes of [ROM](#), 256 kilobytes of programmable ROM, and a 16-bit microprocessor. The smart card uses a serial interface and receives its power from external sources like a card reader. The processor uses a limited instruction set for applications such as cryptography.

The most common smart card applications are:

- Credit cards
- Electronic cash
- Computer security systems
- Wireless communication
- Loyalty systems (like frequent flyer points)
- Banking
- [Satellite TV](#)
- Government identification

Smart cards can be used with a smart-card reader attachment to a [personal computer](#) to authenticate a user. Web browsers also can use smart card technology to supplement Secure Sockets Layer (SSL) for improved security of Internet transactions. [Visa's Smart Card FAQ](#) shows how online purchases work using a smart card and a PC equipped with a smart-card reader. Smart-card readers can also be found in [mobile phones](#) and vending machines.

- [HowStuffWorks.com](#)

The incredible growth of the [Internet](#) has excited businesses and consumers alike with its promise of changing the way we live and work. But a major concern has been just how secure the Internet is, especially when you're sending sensitive information through it. Let's face it, there's a whole lot of information that we don't want other people to see, such as:

- Credit-card information
- Social Security numbers
- Private correspondence
- Personal details
- Sensitive company information
- Bank-account information



E-commerce relies on the ability to send information securely.

Information security is provided on computers and over the Internet by a variety of methods. A simple but straightforward security method is to only keep sensitive information on [removable storage](#) media like [floppy disks](#). But the most popular forms of security all rely on **encryption**, the process of encoding information in such a way that only the person (or computer) with the **key** can decode it.

BIOMETRICS

Several features of people are unique to them. Fingerprints are the most common unique feature used to identify people. The pattern of the blood vessels in a person's retina, or the pattern of the iris are others. Automated face recognition is commonly used by police and security agencies to detect wanted people in crowds.

It is not too hard to map a person's fingerprints or retinal pattern and store the map in a database. When a person seeks authentication, their fingerprint or eye is scanned and mapped. The scan is compared to the genuine stored map in the database. It is impossible to forget your fingerprints or lose your retinal pattern.

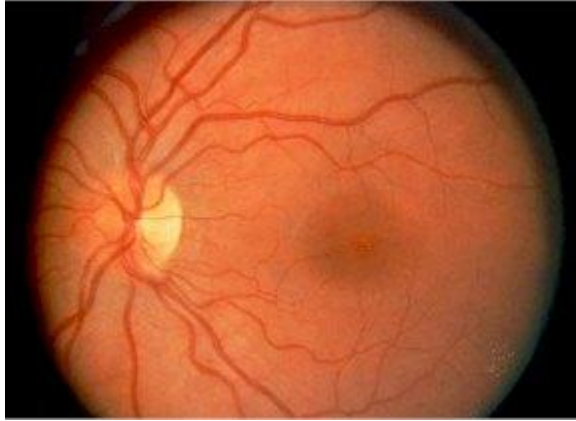
And in case you're wondering it's not easy for villains to chop off your finger or pluck your eye out. A living finger has an electrical activity in it that can be detected. A dead eye loses the blood in its retinal blood vessels and the pattern is different to the eye when it was alive.

Combining biometric and password techniques (e.g. fingerprint scan as well as typing in a secret PIN number) is pretty well foolproof security.

Note that voice recognition or face recognition is not guaranteed to give 100% unique identification of individuals. Some folk are even experimenting with recognising the way a person walks!

Fingerprint recognition can be upset by injuries to the fingers.
Iris patterns, however, hardly ever change during a person's lifetime.

Just so you know what we're talking about on these biometrics
pages



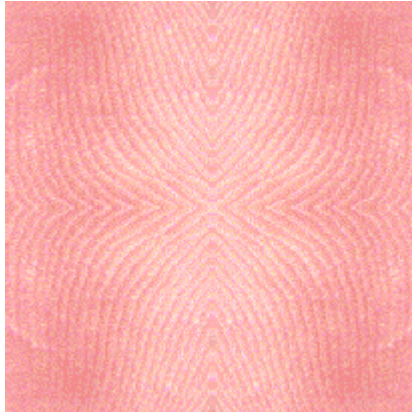
The retina at the back of the eye.
The pattern the blood vessels is unique in each individual.



The iris is the coloured part of the eye around the black pupil.
The patterns in the iris are also unique to each individual.



An iris scanner.
And no, the scanner can't blind you :-)



Fingerprints are unique to each person.



- Biometrics



- [Biometrics](#), facial, voice, fingerprint and eye recognition
- [BBC video](#) and news articles.
- [HowStuffWorks](#)

Authentication

"Authenticity means establishing the user's identity beyond reasonable doubt. Authenticating the user is crucial in many situations, particularly in business and legal matters. A simple example of authentication is user login onto a network. A more advanced example would be the use of encrypted digital signatures in a business transaction" (IBO 2006)

Depending on the sensitivity of the resources you wish to protect will govern what level or how many layers of Authentication are/is used.

- Secret passwords
 - [Password policy](#)
 - It is usually a confirmation to the resource provider of the authenticity of the person based on the fact the user/s know the secret password.
 - Used to allow access to computer systems or resources
 - A major weakness with passwords system can be stolen, accidentally revealed, or forgotten. This is an issue when substantial transactions occur, e.g.. money transfers.

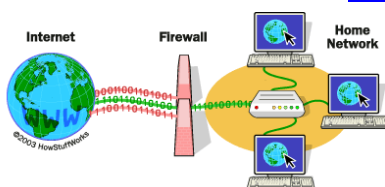
- Personnel history questions: What is your mothers name? or What was your first dogs name? Are often use to verify a user particularity when passwords are forgotten or need to be changed.
- Software solutions IPSEC, Kerberos, XML Signature
- Digital signatures
 - Related [articles](#) to digital signatures and how they have become legally binding.
 - [How it works](#)

Encryption & SSL

- *Encryption* methods can be divided into symmetric key algorithms sometimes called 'private-key cryptography' and asymmetric key algorithms sometimes called 'public-key cryptography'.
 - Encryption methods: read textbook pp. 400-401
 - <http://en.wikipedia.org/wiki/Encryption>
 - An overview of [public encryption](#) & digital signatures, has an input/ouput model.



- SSL is acronym for Secure Sockets Layer
 - SSL is concerned with authentication methods, security issues, and different encryption techniques. This is extremely important for safe and secure [EFT's](#) and bank transactions, protecting personal/customer information, and unwanted [intrusions/hacks](#).
 - [SSL & e-Commerce](#) Article.
 - BBC Article "[Net security software exposed](#)"



Firewalls

- When a computer is connected to the Internet (a public network) then it is at risk from intrusion attacks. Nowadays, with broadband connections the PC even susceptible to attacks because of the constant up time.

- Firewalls have become such an important and necessary tool to fight intrusions. As a result they are common and even PC's have personal firewalls incorporated in its operating software.
- <http://computer.howstuffworks.com/firewall.htm>
- Firewalls can be set-up by either one or the other or a combination of software and hardware.
- Organization firewall policies need to be in place to determine how it should be developed, managed and maintained.

Back ups

If an organisation cannot function without the data then it is imperative that it is backed up!

[Back-up](#) are simply making a copy of the servers and their critical data. Typically they would be carried out (depending on the strategy) daily, weekly and monthly. The copies are usually stored on an external device so that if the server is compromised the data is not.

On our recent visit to IBM in Egypt, they explained how they keep a copy in a safe on the premises, a copy downtown and a third copy at their UK branch.